Privacy Year in Review: Privacy and VoIP Technology

JOHN B. MORRIS, JR.*

ABSTRACT

Voice over internet protocol ("VoIP") technology is increasingly being used throughout the nation. VoIP technology provides for real-time voice communications using an Internet application. Because VoIP technology uses the Internet, security issues arise from third-party attempts at eavesdropping. This technology can also be intercepted under wiretap laws. The means of obtaining these conversations presents new issues for law enforcement agencies because VoIP does not travel along traditional telephone networks and various means of obtaining VoIP are available. Privacy concerns also arise with the vast amount of information that can be obtained from VoIP communications over traditional telephone networks.

I. INTRODUCTION

The usage of Internet-based telephone service – VoIP, "voice over IP (Internet Protocol)," or "voice on the net" technology – is exploding, and VoIP is rapidly becoming a very valuable application for users of broadband (or high-speed) access to the Internet. Although VoIP's penetration into the telephone market is still relatively small, the major providers of VoIP services are seeking tremendous growth. While in many (if not most) cases VoIP services are not the motivating force behind users' decision to pay for broadband access, once users have broadband they often try – and adopt – VoIP services.

As VoIP moves into the mainstream, questions of users' privacy become increasingly important. Although some VoIP services attempt to mimic closely traditional telephone service, the underlying technology is quite different from "plain old telephone service" ("POTS"), and VoIP technology raises new privacy and security issues to consider.

This article first provides a very brief overview of VoIP technology as it is being offered in the marketplace. It then considers,

---

* John B. Morris, Jr. is the Director of Internet Standards, Technology and Policy Project at the Center for Democracy and Technology.

in turn, VoIP privacy issues vis-à-vis (a) hackers and other attackers, (b) the government, and (c) ISPs and VoIP service providers. Finally, it discusses one increasingly important issue related to VoIP technology – the privacy of users' location information.

II. VoIP TECHNOLOGY

VoIP technology is, at its simplest, an Internet application that allows real-time voice communications, in much the same way that "instant messaging" allows real-time text communications. Many, though not all, VoIP services are based on the "Session Initiation Protocol" ("SIP"),[1] which handles the "call setup" process to initiate and terminate calls. In most cases, the entire phone call is carried over the public Internet or over the public Internet to a "gateway" that connects to the traditional phone system. There are, however, a wide array of flavors of VoIP, with sometimes differing security properties and privacy concerns. Among the different flavors of VoIP are:

VoIP within a telephone carrier's network. Technically, many current users of "plain old telephone service" are in fact already unknowingly using VoIP technology, because many traditional telephone carriers (especially long distance carriers such as AT&T, MCI, and Sprint) have implemented "Internet Protocol"-based networks within their existing traditional telephone networks. IP-based networks can be far more efficient than older and more traditional "circuit switched" networks. From the perspective of the end user, this type of VoIP does not raise any significant privacy concerns other than what arises within the traditional telephone network.[2]

"Connected" VoIP provided by an Internet access provider. Led by the cable companies (such as Cox and Comcast) that offer broadband access to their customers, an increasing number of cable- and DSL-based broadband Internet Service Providers are also offering VoIP telephone service to their customers. This type of VoIP is designed and marketed to be as similar as possible to regular "POTS"

---

[1] SIP was created by the Internet Engineering Task Force (IETF), the leading technical standards-setting body for Internet protocols and technologies. Extensive information about the SIP protocol is provided by Professor Henning Schulzrinne at http://www.cs.columbia.edu/sip/.

[2] Because in this context VoIP is not being used over the public Internet but instead is used over the carriers' private IP-based networks, the additional security concerns discussed below are not raised here.

telephone service. By using regular telephone numbers that can reach and be reached by non-VoIP phones, the VoIP service is "connected" to the traditional telephone system. Service providers generally provide a box that plugs into a cable or DSL modem (or an Ethernet network), and into which one or more standard telephones can be plugged.

"Connected" VoIP provided by a third party service provider. Another common model is for a service provider (such as Vonage or AT&T CallVantage) to offer VoIP that is unrelated to the ISP which provides access to the Internet. Like VoIP provided by ISPs, this service also uses regular phones and phone numbers and is intended to be as similar as possible to POTS.

"Computer-to-computer" VoIP provided by a third party service provider. Some VoIP providers (such as Pulver.com's Free World Dialup and Skype) focus their core service on facilitating voice communications between computer users on the Internet, without necessarily connecting to the traditional phone system. This type of service does not necessarily use phone numbers or regular phones. Typically, the service is run through a computer with headphones or a VoIP phone connected to the computer or network. These services are usually free for computer-to-computer calls.

Self-provided "computer-to-computer" VoIP. VoIP can be implemented using public standards and protocols, entirely without a "service provider." Thus, two or more individuals or companies could connect to each other using software entirely controlled by the users (and not by any outside "provider").

These different models of VoIP service raise, in many cases, different privacy and security concerns (and indeed, even within one type of VoIP service identified above, there are important technical differences in how each individual service is provided). Some of the differences are highlighted below.

III. VoIP AND SECURITY FROM THIRD PARTY ATTACK

Because for most VoIP communications some or all of the communication travels over the public Internet, VoIP faces an array of security issues similar to that found with most Internet communications, and some of the security threats implicate privacy concerns. Among the concerns that will arise are "VoIP spam" and scams using spoofed (or faked) Caller-ID information showing the supposed origin of a VoIP call. From a privacy perspective, it is at least theoretically possible that third parties (meaning someone other than a government or service provider) could intercept VoIP

communications as they traverse the Internet. The risk of such eavesdropping is reasonably low and roughly the same as the risk of a third party being able to intercept an e-mail. But, the risk for most VoIP services today is greater than the comparable risk of an unauthorized third party interception of a traditional POTS phone call (which generally travel only over closed, non-public networks). As a practical matter, however, this type of privacy risk is currently low for VoIP calls.

Some VoIP services – most prominently including the Skype service – go a great distance toward eliminating this risk by encrypting the voice communications. Thus, if someone were able to intercept Skype-based VoIP communications, the communication would be unintelligible. Moreover, Skype's encryption is designed so that even the providers of the Skype service itself would be unable to decrypt a Skype communication.[3]

VoIP providers are aware of and are trying to address security concerns surrounding VoIP communications.[4] As more and more corporations use VoIP technology for both internal and external voice calls, it is likely that VoIP services will offer increasingly secure options for VoIP calls.

IV. VOIP AND WIRETAPPING

Entirely apart from the security concerns discussed above, there is no question that VoIP communications can – from both a technical and legal perspective – be intercepted pursuant to a court-issued wiretap order. Legally, VoIP communications (as well as any other Internet communications) can be intercepted pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[5] the Electronic Communications Privacy Act of 1986 ("ECPA"),[6] or the Foreign Intelligence Surveillance Act of 1978 ("FISA").[7] Just as a

---

[3] On the other hand, although the voice portion of Skype service is more secure than most other currently available VoIP service offerings, call setup information is less secure on the Skype system than with most other VoIP services. Skype's call setup is done on a "peer-to-peer" basis, and thus it would be fairly easy for a third party to know that one particular Skype user is trying to place a call to another particular Skype user.

[4] *See, e.g., Industry group sets out to make VoIP secure*, Network World Fusion (Mar. 29, 2005), *available at* http://www.nwfusion.com/news/2005/ 0329indusgroup.html.

[5] Pub. L. No. 90-351, 82 Stat. 212 (1968).

[6] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

traditional telephone company (or anyone else, such as an apartment building landlord) is obligated to cooperate with a court interception order, so too is an ISP or VoIP service provider obligated to cooperate.

As a technical matter, law enforcement agencies can intercept VoIP communications. As compared to interceptions of traditional POTS calls, however, there are three important "big picture" differences with the interception of VoIP calls. First, unlike with traditional telephone networks (which are generally homogeneous and slow to evolve), there are many flavors of VoIP, and thus differing formats and protocols used within the differing VoIP services. Second, unlike with the traditional telephone networks (which can generally format an intercepted phone call into one standardized form), the law enforcement agencies themselves may need to be able to understand the differing VoIP formats. And third, unlike with the traditional telephone networks (where law enforcement usually needs to order only a single company to provide intercepted communications), law enforcement may need to obtain information about an intercepted VoIP call from two or more different companies at the same time. For example, law enforcement might need to obtain the "call setup" information from one source, and the call content itself from another source.

All of these differences have led the United States Department of Justice and the Federal Bureau of Investigation to seek to extend the Communications Assistance for Law Enforcement Act ("CALEA")[8] to Internet communications in general and to VoIP communications in particular. In March of 2004, the law enforcement agencies filed a petition with the Federal Communications Commission ("FCC") asking that CALEA apply to certain types of VoIP service.[9] Despite strong objections raised in comments by a wide variety of parties, the FCC generally agreed with law enforcement, and the Commission issued a Notice of Proposed Rulemaking ("NPRM") extending CALEA to the Internet and certain VoIP communications.[10]

---

[7] 50 U.S.C. §§ 1801-1843.

[8] Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-10 and 47 U.S.C. § 229).

[9] Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, Federal Communications Commission, RM-10865 (filed Mar. 10, 2004), *available at* http://www.cdt.org/digi_tele/20040310fbipetition.pdf.

[10] *In the Matter of Communications Assistance for Law Enforcement Act, Notice of Proposed Rulemaking*, ET Docket No. 04-295, RM-10865 (released Aug. 9, 2004) ("NPRM"), *published* 69 Fed. Reg. 56,976 (Sept. 23, 2004).

Extensive comments were filed by numerous parties objecting to the NPRM on numerous grounds, and the FCC has not yet finalized the rules proposed in the NPRM. Among the main concerns about the NPRM is the fact that the extension of CALEA to the Internet and VoIP will give the Federal Bureau of Investigation the ability to dictate specific design obligations, which providers of VoIP services must meet to be able to do business in the United States. Commenters to the FCC argued that the ability of law enforcement to impose technology design mandates would chill technological innovation and drive technology development out of the U.S.[11]

Among the privacy concerns implicated by law enforcement's attempt to force VoIP communications into the CALEA model is that law enforcement will receive far more information, and far more private information, with VoIP interceptions as compared with traditional POTS interceptions. For example, with a "pen register" or "trap and trace" order in the traditional phone system, law enforcement receives details about when a phone call was initiated, but receives neither the content of the call nor any information about the call. If CALEA is imposed onto VoIP calls, it is likely that law enforcement would also seek to obtain the topic subject of the VoIP call (because, like e-mail, the subject of a proposed VoIP call using the SIP protocol can be transmitted at the start of the call).

It is not clear whether law enforcement's attempt to extend CALEA to VoIP calls will be successful. There are many legal doubts about the FCC's authority to take that action, and any final rule extending CALEA will almost certainly be challenged in court. It is possible that Congress will effectively pre-empt the FCC's rulemaking and directly address questions concerning the wiretapping of VoIP calls.

V. VoIP Privacy and Service Providers

There are strong protections in the traditional telephone system to prevent service providers from intercepting and listening to their

---

[11] Many of the objections are discussed in the Joint Statement of Industry and Public Interest Groups on CALEA Notice of Proposed Rulemaking and the Joint Reply Comments of Industry and Public Interest Groups on CALEA Notice of Proposed Rulemaking. See Joint Statement of Industry and Public Interest Groups on CALEA Notice of Proposed Rulemaking (filed with the FCC on Nov. 8, 2004), *available at* http://www.cdt.org/digi_tele/20041108intpubint.pdf; Joint Reply Comments of Industry and Public Interest Groups on CALEA Notice of Proposed Rulemaking (filed on Dec. 21, 2004), *available at* http://www.cdt.org/digi_tele/20041221joint.pdf.

customers' calls. Such expectations of privacy have and will carry over to the VoIP world, and it appears unlikely that ISPs or VoIP service providers will intentionally intercept customers' VoIP calls.

Having said that, however, there nevertheless are significant privacy concerns vis-à-vis service providers that would flow from the extension of CALEA discussed above. If CALEA is extended to VoIP communications, there is a significant risk that ISPs and VoIP service providers would be *forced* by law enforcement to develop the capability (within the service providers' networks) to eavesdrop on their customers and determine exactly what type of Internet communication the customer is utilizing at any given time.

Thus, the private service providers would have to develop an internal capability to snoop on their own customers – a capability that the providers do not currently have. This raises at least two privacy risks. First, it is possible that the services providers would be tempted to use the interception capability for their own commercial purposes.[12] Second, there is an unavoidable risk that rogue employees of the service providers could abuse the internal surveillance capability.

VI. PRIVACY OF LOCATION INFORMATION

Although not uniquely tied to VoIP, there is increasingly cause for concern about the privacy of information about the location of telephone and Internet users. As communications (including cellular and other mobile communications) increasingly use VoIP technology (and Internet Protocol technology more generally), there is an increasing use of location information. This location information is often generated by cellular tower triangulation, where location is measured based on the signal strength to multiple cellular towers. The location is increasingly being determined by using internal GPS (global positioning system) technology within laptops and mobile telephones. In some parts of the world wireless services providers are already "pushing" advertisements to phones based on the location of the phone (and thus the location of the user).

---

[12] Although most service providers have generally disavowed any intention to snoop on their customers, at least two examples (both involving small service providers) indicate that the concern is well founded. *See* United States v. Councilman, 373 F.3d 197 (1st Cir. 2004) (a small service provider used intercepted e-mails for the provider's commercial benefit); Consent Decree, In the Matter of Madison River Communications, LLC and affiliated companies, FCC File No. EB-05-IH-0110 (Mar. 3, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf (a small ISP blocked its customers' VoIP calls because the ISP, owned by a traditional telephone company, did not want the customers to use VoIP telephone service in lieu of traditional service).

The technical community has developed technology to protect location information in Internet Protocol-based communications. The "geopriv" working group of the Internet Engineering Task Force ("IETF") is in the process of finalizing a protocol that would require any transmission of location using IETF protocols also to transmit privacy rules that must be honored.[13] Although IETF protocols are voluntary standards, the leading "third generation" wireless standards bodies have indicated that they intend to incorporate the IETF's geopriv protocol when it is completed, and thus there is a reasonable prospect that users will have a significant element of control over the use of their location information.

A significant exception to the concept that users will control their location information arises in the emergency or "E-911" context, in which service providers face obligations under FCC rules to be able to provide the location of a user who places a 911 emergency call. As part of its location privacy work, the IETF is working to facilitate the secure delivering of location information in the event of an emergency.[14]

VII. CONCLUSION

Although VoIP technology has existed for more than ten years, it is only in the past two years that its use has entered the mainstream. VoIP is therefore still very much a new and evolving technology. As such, all of the privacy problems have not yet arisen, nor have all of the possible privacy protections yet been deployed. Many of the privacy concerns discussed above are somewhat theoretical, or at least have yet to develop into broad problems with widespread abuses. Many in the VoIP technology development community are committed to strong privacy protections, and so there is a reasonable chance that VoIP will prove to be a fairly privacy-friendly technology.

---

[13] *See* J. Morris et al., *Geopriv Requirements*, RFC 3693 (February 2004), *available at* http://www.ietf.org/rfc/rfc3693.txt.

[14] *See generally Emergency Context Resolution with Internet Technologies (ecrit)*, http://www.ietf.org/html.charters/ecrit-charter.html (last modified March 7, 2005).